

JOSEPH H. HUNT
Assistant Attorney General
Civil Division
GUSTAV W. EYLER
Acting Director
KENDRACK D. LEWIS
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice,
Civil Division
P.O. Box 386
Washington, DC 20044-0386
Telephone: (202) 353-3881
Fax: (202) 514-8742
kendrack.lewis@usdoj.gov

MONIQUE F. EINHORN
RYAN M. MEHM
Attorneys
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-3289
meinhorn@ftc.gov
rmehm@ftc.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,
vs.

UNIXIZ, Inc., a corporation doing business
as i-Dressup.com, and

ZHIJUN LIU and XICHEN ZHANG,
individually and as officers of UNIXIZ,
Inc.

Defendants.

Case No. 5:19-cv-2222

**STIPULATED ORDER FOR CIVIL
PENALTIES, PERMANENT
INJUNCTION, AND OTHER RELIEF**

Plaintiff, the United States of America, acting upon notification and on behalf of the Federal Trade Commission (“Commission”), filed its Complaint for Permanent Injunction and Other Equitable Relief (“Complaint”), in this matter, pursuant to Sections 13(b) and 16(a)(1) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b) and 56(a)(1), the Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6502(c) and 6505(d), and the Commission’s Children’s Online Privacy Protection Rule (“COPPA Rule”), 16 C.F.R. Part 312. Defendants have waived service of the summons and the Complaint. Plaintiff and Defendants stipulate to the entry of this Stipulated Order for Permanent Injunction and Civil Penalty Judgment (“Order”) to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint charges that Defendants violated COPPA and the FTC Act by failing to include information required by COPPA in i-Dressup’s notice of information practices; failing to provide sufficient direct notice of their information practices to Parents; failing to Obtain Verifiable Parental Consent; and failing to delete Online Contact Information of a Parent after having failed to obtain consent.
3. Defendants neither admit nor deny any of the allegations in this Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendants admit the facts necessary to establish jurisdiction.
4. Defendants waive any claim they may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agree to bear their own costs and attorney fees.

- 1 5. Defendants and Plaintiff waive all rights to appeal or otherwise challenge or contest the
2 validity of this Order.

3 **DEFINITIONS**

4 For the purpose of this Order, the following definitions apply:

- 5 A. “Child” or “Children” means an individual or individuals under the age of 13.
6
7 B. Except for purposes of Parts III and IV of this Order, “Collects” or “Collect” or
8 “Collection” or “Collected” or “Collecting” means the gathering of any Personal
9 Information from a Child by any means, including but not limited to:
10 1. Requesting, prompting, or encouraging a Child to submit Personal Information
11 online;
12 2. Enabling a Child to make Personal Information publicly available in identifiable
13 form; or
14 3. Passive tracking of a Child online.
15
16 C. “Covered Incident” means any instance in which any United States federal, state, or local
17 law or regulation requires a Covered Business or Individual Defendant to notify any U.S.
18 federal, state, or local government entity that information Collected or received, directly
19 or indirectly, by a Covered Business from or about an individual consumer was, or is
20 reasonably believed to have been, accessed or acquired without authorization.
21
22 D. “Covered Business” means Corporate Defendant and any business that Individual
23 Defendants, individually, collectively, or in any combination, control, directly or
24 indirectly.

1 E. "Covered Information" means any "Personal Information" as defined in this Order and
2 any of the following individually identifiable information from or about an individual
3 consumer, obtained online, including:

- 4 1. Date of Birth;
- 5 2. Other government-issued identification numbers, such as a driver's license
6 number, military identification number, passport number, or other personal
7 identification number;
- 8 3. Financial institution account number;
- 9 4. Credit or debit card information; or
- 10 5. Authentication credentials, such as a username or password.

11 F. "Defendants" means all of the Individual Defendants and the Corporate Defendant,
12 individually, collectively, or in any combination.

- 13 1. "Corporate Defendant" means Unixiz, Inc., d/b/a i-Dressup.com, and its
14 successors and assigns.
- 15 2. "Individual Defendants" means Zhijun Liu and Xichen Zhang.

16 G. Except for purposes of Part VII of this Order, "Disclose" or Disclosure" or "Disclosed"
17 means, with respect to Personal Information:

- 18 1. The release of Personal Information Collected by an Operator from a Child in
19 identifiable form for any purpose, except where an Operator provides such
20 information to a Person who provides Support For The Internal Operations Of
21 The Web Site Or Online Service; and
- 22 2. Making Personal Information Collected by an Operator from a Child publicly
23 available in identifiable form by any means, including but not limited to a public
24

posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

H. “Internet” means collectively the myriad of computer and telecommunication facilities, including equipment and operating software, which comprises the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

I. “Obtaining Verifiable Parental Consent” or “Obtain Verifiable Parental Consent” means making any reasonable effort (taking into consideration available technology) to ensure that before Personal Information is Collected from a Child, a Parent of the Child:

1. Receives notice of the Operator’s Personal Information Collection, use, and Disclosure practices; and
2. Authorizes any Collection, use, and/or Disclosure of the Personal Information.

J. “Online Contact Information” means an email address or any other substantially similar identifier that permits direct contact with a Person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat identifier.

K. “Operator” means any person who operates a Web site located on the Internet or an online service and who Collects or maintains Personal Information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is Collected or maintained, or offers products or services for sale through the Web site or online service, where such Web site or online service is operated for

1 commercial purposes involving commerce among the several States, or with one (1) or
2 more foreign nations; in any territory of the United States or in the District of Columbia,
3 or between any such territory and another such territory or any State or foreign nation; or
4 between the District of Columbia and any State, territory, or foreign nation.

5 L. Except for purposes of Part IX of this Order, “Parent” includes a legal guardian.

6 M. “Person” means any individual, partnership, corporation, trust, estate, cooperative,
7 association, or other entity.

8 N. “Personal Information” means individually identifiable information about an individual
9 Collected online, including:
10

- 11 1. A first and last name;
- 12 2. A home or other physical address including street name and name of a city or
13 town;
- 14 3. Online Contact Information, as defined in 16 C.F.R. § 312.2;
- 15 4. A screen or user name where it functions in the same manner as online contact
16 information, as defined in 16 C.F.R. § 312.2;
- 17 5. A telephone number;
- 18 6. A Social Security number;
- 19 7. A persistent identifier that can be used to recognize a user over time and across
20 different Web sites or online services. Such persistent identifier includes, but is
21 not limited to, a customer number held in a cookie, an Internet Protocol (IP)
22 address, a processor or device serial number, or unique device identifier;
- 23 8. A photograph, video, or audio file where such file contains a Child’s image or
24 voice;
- 25
- 26
- 27
- 28

9. Geolocation information sufficient to identify street name and name of a city or town; or

10. Information concerning the Child or the Parents of that Child that the Operator Collects online from the Child and combines with an identifier described in this section.

O. "Release Of Personal Information" means the sharing, selling, renting, or transfer of Personal Information to any Third Party.

P. "Support For The Internal Operations Of The Web Site or Online Service" means:

1. Those activities necessary to:

a. Maintain or analyze the functioning of the Web site or online service;

b. Perform network communications;

c. Authenticate users of, or personalize the content on, the Web site or online service;

d. Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

e. Protect the security or integrity of the user, Web site, or online service;

f. Ensure legal or regulatory compliance; or

g. Fulfill a request of a Child as permitted by 16 C.F.R. §§ 312.5(c)(3) and (4) of COPPA;

2. So long as the information Collected for the activities listed in paragraphs (1)(a)-(g) of this definition is not used or Disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

1 Q. "Third Party" means any Person who is not:

- 2 1. An Operator with respect to the Collection or maintenance of Personal
3 Information on the Web site or online service; or
4
5 2. A Person who provides support for the internal operations of the Web site or
6 online service and who does not use or Disclose information protected under 16
7 C.F.R. Part 312 for any other purpose.

8 R. "Web Site Or Online Service Directed To Children" means a commercial Web site or
9 online service, or portion thereof, that is targeted to Children.

- 10 1. In determining whether a Web site or online service, or a portion thereof, is
11 directed to Children, the Commission will consider its subject matter, visual
12 content, use of animated characters or Child-oriented activities and incentives,
13 music or other audio content, age of models, presence of Child celebrities or
14 celebrities who appeal to Children, language or other characteristics of the Web
15 site or online service, as well as whether advertising promoting or appearing on
16 the Web site or online service is directed to children. The Commission will also
17 consider competent and reliable empirical evidence regarding audience
18 composition, and evidence regarding the intended audience.
19
20 2. A Web site or online service shall be deemed directed to Children when it has
21 actual knowledge that it is Collecting Personal Information directly from users of
22 another Web Site Or Online Service Directed To Children.
23
24 3. A Web site or online service that is directed to Children under this criteria set
25 forth in paragraph (1) of this definition, but that does not target Children as its
26 primary audience, shall not be deemed directed to Children if it:
27
28

a. Does not Collect Personal Information from any visitor prior to Collecting age information; and

b. Prevents the Collection, use, or Disclosure of Personal Information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of 16 C.F.R. Part 312.

4. A Web site or online service shall not be deemed directed to Children solely because it refers or links to a commercial Web site or online service directed to Children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

ORDER

I. INJUNCTION CONCERNING THE COLLECTION OF PERSONAL INFORMATION

IT IS ORDERED that Defendants and Defendants' officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with being an Operator of any Web Site Or Online Service Directed To Children or of any Web site or online service with actual knowledge that it is Collecting or maintaining Personal Information from a Child, are hereby permanently restrained and enjoined from violating the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, including, but not limited to:

- A. Failing to provide sufficient notice on its Web site or online services of the Personal Information it Collects, or is Collected on their behalf, online from Children, how it uses such information, its Disclosure practices, and all other required content;
- B. Failing to provide sufficient direct notice to Parents of the Personal Information Defendants Collect, or Personal Information that has been Collected on Defendants'

1 behalf, online from Children, how it uses such information, its Disclosure practices, and
2 all other required content;

3 C. Failing to Obtain Verifiable Parental Consent using a method reasonably calculated to
4 ensure that the Person providing consent is the Child's Parent, and failing to Obtain
5 Verifiable Parental Consent for some under-13 users despite Collecting Personal
6 Information from them;

7 D. Failing to delete Online Contact Information of the Parent after having failed to Obtain
8 Verifiable Parental Consent; and

9 E. Failing to establish and maintain reasonable procedures to protect the confidentiality,
10 security, and integrity of Personal Information Collected from Children.

11 A copy of the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, is attached
12 hereto as appendix A.
13

14
15 **II. MONETARY JUDGEMENT FOR CIVIL PENALTY**

16 IT IS FURTHER ORDERED that:

17 A. Judgement in the amount of thirty-five thousand dollars (\$35,000) is entered in favor of
18 Plaintiff against Defendants, jointly and severally, as a civil penalty.

19 B. Defendants are ordered to pay to Plaintiff, by making payment to the Treasurer of the
20 United States, thirty-five thousand dollars (\$35,000), which, as Defendants stipulate, their
21 undersigned counsel holds in escrow for no purpose other than payment to Plaintiff.

22 Such payment must be made within seven (7) days of entry of this Order by electronic
23 fund transfer in accordance with instructions previously provided by a representative of
24 Plaintiff.
25
26
27
28

III. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

- A. Defendants relinquish dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.
- B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission, including in a proceeding to enforce its rights to any payment or monetary judgement pursuant to this Order.
- C. Defendants agree that the judgment represents a civil penalty owed to the government of the United States, is not compensation for actual pecuniary loss, and, therefore, as to the Individual Defendants, it is not subject to discharge under the Bankruptcy Code pursuant to 11 U.S.C. § 523(a)(7).
- D. Defendants acknowledge that their Taxpayer Identification Numbers, which Defendants must submit to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. §7701.

IV. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that each Covered Business shall not transfer, sell, share, collect, maintain, or store Covered Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program (“Information Security Program”) that is designed to protect the security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

- 1 A. Document in writing the content, implementation, and maintenance of the Information
2 Security Program;
- 3 B. Designate a qualified employee or employees to coordinate and be responsible for the
4 Information Security Program;
- 5 C. Assess and document, at least once every twelve months and promptly following a
6 Covered Incident, internal and external risks to the security, confidentiality, or integrity
7 of Covered Information that could result in the unauthorized Disclosure, misuse, loss,
8 alteration, destruction, or other compromise of such information;
- 9 D. Design, implement, and document safeguards that address the internal and external risks
10 each Covered Business identifies to the security, confidentiality, or integrity of Covered
11 Information identified in response to sub-Provision IV.C. Each safeguard shall take into
12 account the sensitivity of Covered Information at issue;
- 13 E. Assess, at least once every twelve months and promptly following a Covered Incident,
14 the sufficiency of any safeguards in place to address the risks to the security,
15 confidentiality, or integrity of Covered Information. Each such assessment must evaluate
16 safeguards in each area of relevant operation, including: (1) employee training and
17 management; (2) information systems, such as network and software design, information
18 processing, storage, transmission, and disposal; and (3) prevention, detection, and
19 response to attacks, intrusions, or other systems failures;
- 20 F. Test and monitor the effectiveness of the safeguards at least once every twelve months
21 and promptly following a Covered Incident, and modify the Information Security
22 Program based on the results;
- 23
24
25
26
27
28

1 G. Select and retain service providers capable of safeguarding Covered Information they
2 receive from each Covered Business, and contractually require service providers to
3 implement and maintain safeguards for Covered Information; and

4 H. Evaluate and adjust the Information Security Program in light of any changes to its
5 operations or business arrangements, a Covered Incident, or any other circumstances that
6 Defendants know or have reason to know may have an impact on the effectiveness of the
7 Information Security Program. At a minimum, Defendants must evaluate the Information
8 Security Program at least once every twelve months.

9
10 **V. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY**

11 IT IS FURTHER ORDERED that in connection with compliance with Provision IV of
12 this Order titled Mandated Information Security Program, Defendants must obtain initial and
13 biennial assessments ("Assessments"):

14
15 A. The Assessments must be obtained from a qualified, objective, independent third-party
16 professional ("Assessor"), who uses procedures and standards generally accepted in the
17 profession. The Assessor preparing such Assessments must be: an individual qualified
18 as a Certified Information System Security Professional (CISSP) or as a Certified
19 Information Systems Auditor (CISA); an individual holding Global Information
20 Assurance Certification (GIAC) from the SANS Institute; or a qualified individual or
21 entity approved by the Associate Director for Enforcement, Bureau of Consumer
22 Protection, Federal Trade Commission.
23
24
25
26
27
28

- 1 B. The reporting period for the Assessments must cover: (1) the first 180 days after the
 2 issuance date of the Order for the initial Assessment; and (2) each 2-year period
 3 thereafter for ten (10) years after issuance of the Order for the biennial Assessments.
- 4 C. Each Assessment must: (1) determine whether each Covered Business has implemented
 5 and maintained Provision IV of this Order titled Mandated Information Security
 6 Program; (2) assess the effectiveness of each Covered Business's implementation and
 7 maintenance of sub-Provisions IV.A-H; and (3) identify any gaps or weaknesses in the
 8 Information Security Program.
- 9 D. Each Assessment must be completed within sixty (60) days after the end of the reporting
 10 period to which the Assessment applies. Unless otherwise directed by a Commission
 11 representative in writing, Defendants must submit the initial Assessment to the
 12 Commission within ten (10) days after the Assessment has been completed via email to
 13 DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate
 14 Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission,
 15 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin:
 16 FTC v. Unixiz, Inc. All subsequent biennial Assessments shall be retained by Defendants
 17 until the order is terminated and provided to the Associate Director for Enforcement
 18 within ten (10) days of request.

21 **VI. PROHIBITION AGAINST MISREPRESENTATIONS TO THE ASSESSOR**

22 IT IS FURTHER ORDERED that Defendants, whether acting directly or indirectly, in
 23 connection with any Assessment required by Provision V of this Order titled Information
 24 Security Assessments by a Third Party, must not misrepresent in any manner, expressly or by
 25 implication, any fact material to the Assessor's: (1) determination of whether each Covered
 26
 27
 28

1 Business has implemented and maintained Provision IV of this Order titled Mandated
 2 Information Security Program; (2) assessment of the effectiveness of the implementation and
 3 maintenance of sub-Provisions IV.A-H; or (3) identification of any gaps or weaknesses in the
 4 Information Security Program.

5 **VII. ANNUAL CERTIFICATION**

6
 7 IT IS FURTHER ORDERED that in connection with compliance with Provision IV of
 8 this Order titled Mandated Information Security Program, Defendants shall:

9 A. One year after the issuance date of this Order, and each year thereafter for a period of ten
 10 (10) years, provide the Commission with a certification from a senior corporate manager,
 11 or, if no such senior corporate manager exists, a senior officer of each Covered Business
 12 responsible for each Covered Business's Information Security Program that: (1) each
 13 Covered Business has established, implemented, and maintained the requirements of this
 14 Order; (2) each Covered Business is not aware of any material noncompliance that has
 15 not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief
 16 description of any Covered Incident. The certification must be based on the personal
 17 knowledge of the senior corporate manager, senior officer, or subject matter experts upon
 18 whom the senior corporate manager or senior officer reasonably relies in making the
 19 certification.
 20

21
 22 B. Unless otherwise directed by a Commission representative in writing, submit all annual
 23 certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or
 24 by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement,
 25 Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue
 26 NW, Washington, DC 20580. The subject line must begin: FTC v. Unixiz, Inc.
 27
 28

VIII. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendants obtain acknowledgments of receipt of this Order:

- A. Each Defendant, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 5 years after entry of this Order, each Individual Defendant for any business that such Defendant, individually or collectively with any other Defendants, is the majority owner or controls directly or indirectly, and each Corporate Defendant, must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Section titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which a Defendant delivered a copy of this Order, that Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

IX. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendants make timely submissions to the Commission:

A. One year after entry of this Order, each Defendant must submit a compliance report, sworn under penalty of perjury.

1. Each Defendant must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and Plaintiff may use to communicate with Defendant; (b) identify all of that Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Defendant (which Individual Defendants must describe if they know or should know due to their own involvement); (d) describe in detail whether and how that Defendant is in compliance with each Section of this Order; (e) provide a copy of each different version of any privacy notice posted on each Web site or online service operated by Defendants or sent to Parents of Children that register on each Web site or online service; (f) describe in detail the methods used to Obtain Verifiable Parental Consent prior to any Collection, use, and/or Disclosure of Personal Information from Children through any Web site or online service; (g) describe in detail the means provided for Parents to review the Personal Information Collected from their Children and to refuse to permit its further use

1 or maintenance; and (h) provide a copy of each Order Acknowledgment obtained
2 pursuant to this Order, unless previously submitted to the Commission.

3 2. Additionally, each Individual Defendant must: (a) identify all telephone
4 numbers and all physical, postal, email and Internet addresses, including all
5 residences; (b) identify all business activities, including any business for which
6 such Defendant performs services whether as an employee or otherwise and any
7 entity in which such Defendant has any ownership interest; and (c) describe in
8 detail such Defendant's involvement in each such business, including title, role,
9 responsibilities, participation, authority, control, and any ownership.
10

11 B. For ten (10) years after entry of this Order, each Defendant must submit a compliance
12 notice, sworn under penalty of perjury, within fourteen (14) days of any change in the
13 following:
14

15 1. Each Defendant must report any change in: (a) any designated point of contact;
16 or (b) the structure of any Corporate Defendant or any entity that Defendant has
17 any ownership interest in or controls directly or indirectly that may affect
18 compliance obligations arising under this Order, including: creation, merger, sale,
19 or dissolution of the entity or any subsidiary, parent, or affiliate that engages in
20 any acts or practices subject to this Order.

21 2. Additionally, each Individual Defendant must report any change in: (a) name,
22 including aliases or fictitious name, or residence address; or (b) title or role in any
23 business activity, including any business for which such Defendant performs
24 services whether as an employee or otherwise and any entity in which such
25
26
27
28

Defendant has any ownership interest, and identify the name, physical address, and any Internet address of the business or entity.

- C. Each Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Defendant within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: FTC v. Unixiz, Inc.

X. RECORDKEEPING

IT IS FURTHER ORDERED that Defendants must create certain records for (ten) 10 years after entry of the Order, and retain each such record for (five) 5 years. Specifically, Corporate Defendant in connection with any Web site or online service and each Individual Defendant for any business that such Defendant, individually or collectively with any other Defendants, is a majority owner or controls directly or indirectly, must create and retain the following records:

- A. accounting records showing the revenues from all goods or services sold;

- B. personnel records showing, for each Person providing services, whether as an employee or otherwise, that Person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
 - C. records of all consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a Third Party, and any response;
 - D. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and
 - E. a copy of each materially different form, page, or screen created, maintained, or otherwise provided by Defendants through which Personal Information is Collected through any Web site or online service, and a copy of each materially different document containing any representation regarding Collection, use, and Disclosure practices pertaining to Personal Information Collected through such Web site or online service.
- Each webpage copy shall be accompanied by the URL of the webpage where the material was posted online. Electronic copies shall include all text and graphic files, audio scripts, and other computer files used in presenting information on the Internet.

XI. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendants' compliance with this Order, including any failure to transfer any assets as required by this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or Plaintiff, each Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission and Plaintiff are also authorized to obtain discovery, without further leave of court, using any

of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

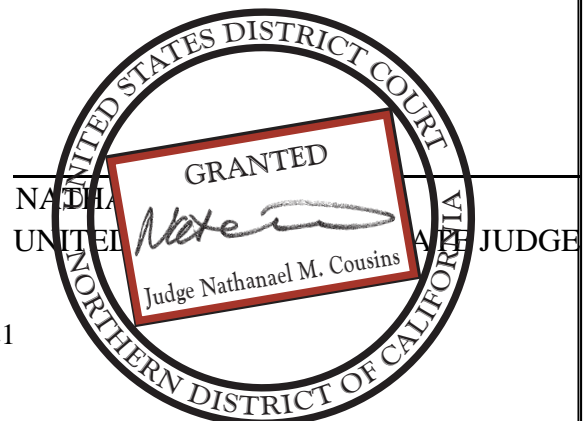
- B. For matters concerning this Order, the Commission and Plaintiff are authorized to communicate directly with each Defendant. Defendant must permit representatives of the Commission and Plaintiff to interview any employee or other Person affiliated with any Defendant who has agreed to such an interview. The Person interviewed may have counsel present.
- C. The Commission and Plaintiff may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Defendants or any individual or entity affiliated with Defendants, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.
- D. Upon written request from a representative of the Commission or Plaintiff, any consumer reporting agency must furnish consumer reports concerning Individual Defendants, pursuant to Section 604(1) of the Fair Credit Reporting Act, 15 U.S.C. §1681b(a)(1).

XII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

All parties have consented to the jurisdiction of a magistrate judge under 28 U.S.C. section 636(c).

SO ORDERED this 2nd day of May, 2019.



1
2 **SO STIPULATED AND AGREED:**

3 **FOR PLAINTIFF UNITED STATES OF AMERICA**

4 JOSEPH H. HUNT
5 Assistant Attorney General
6 Civil Division

7 GUSTAV W. EYLER
8 Acting Director

9 /S/
10 KENDRACK D. LEWIS
11 Trial Attorney
12 Consumer Protection Branch
13 U.S. Department of Justice, Civil Division
14 P.O. Box 386
15 Washington, DC 20044-0386
16 Tel: (202) 353-0386
17 kendrack.lewis@usdoj.gov

18 **FOR THE FEDERAL TRADE COMMISSION**

19 MANEESHA MITHAL
20 Associate Director
21 Division of Privacy and Identity Protection

22 ROBERT SCHOSHINSKI
23 Assistant Director
24 Division of Privacy and Identity Protection

25 /S/
26 MONIQUE F. EINHORN
27 RYAN M. MEHM
28 Attorneys
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
Tel: (202) 326-2575
Fax: (202) 326-3062
meinhorn@ftc.gov
rmehm@ftc.gov

FOR DEFENDANTS

STACEY BRANDENBURG

ZwillGen PLLC

1900 M Street, NW

Suite 250

Washington, DC 20036

Tel: (202) 706-5220

stacey@zwillgen.com

Counsel for Unixiz, Inc. and Zhijun Liu and Xichen Zhang

Date: _____

KANDI PARSONS

ZwillGen PLLC

1900 M Street, NW

Suite 250

Washington, DC 20036

Tel: (202) 706-5213

Kandi@zwillgen.com

Counsel for Unixiz, Inc. and Zhijun Liu and Xichen Zhang

Date: _____

DEFENDANTS

ZHIJUN LIU

Individually, and as CEO and CFO of Unixiz, Inc.

Date: _____

XICHEN ZHANG

Individually, and as Secretary of Unixiz, Inc.

Date: _____